Detection of Abnormalities in MANETs

Wenye Wang, ECE Department, NC State University

1 Fundamental Limitations of Today's Solutions

Abnormalities in MANETs can be malicious attacks or selfish nodes which can affect network architecture and network operation significantly.

1.1 No Detection of Abnormalities

Without detection of abnormalities, secure routing can be considered as a *proactive* solution. Recently many secure routing protocols, such as ARAN, Adriadne, SAODV, SRP, SEAD, have been proposed to protect multihop wireless networks from malicious attacks that interrupt routing or [1, 2]. Clearly, there are two *distinct* objectives:

- Security is a goal: In this category, the idea is to show how attacks against ad-hoc and sensor networks, and analyze the security of all routing protocols. The objective is to design/examine attacks and develop countermeasures [3].
- Routing is a goal: The objective of these works is to design/modify current routing protocols, but adding new security features to prevent the routing from attacks and interruption.

For both directions, security analysis has been addressed along with peer-to-peer networking architecture for MANETs and sensor networks. In short, there are 10 attacks addressed by most of these works, except each work discusses one or more specific attacks that are not covered by others: *spoofing of IP address, forging of route request, forging of route reply, injecting route reply without receiving a route request, replay attack, rushing attacks, generating false errors, jamming, man-in-the-middle attack, modifying node list on a route request.* Almost all of these works are based on simulations and qualitative explanation without implementations in MANETs. An intuitive question is whether these solutions, or *at least* one solution is feasible to MANETs. To the best of our knowledge, NIST (National Institute of Standard and Technology) and UMBC developed the open source code of SAODV, which is also called SecAODV with IPv6. We found a technical report of their implementation with very few testing results [4]. In order to understand the functionalities of SecAODV, we used the open source code available at NIST and implemented on our testbed. Surprising, we found that the packet looses are in between 90%-100%! This simply tells us: a protocol could be very secure (from analysis), but might not be able to delivery data. The reasons for such a result are not fully explored which maybe one or combined factors, such as bugs in the code, optimization problem, or protocol design. However, it advises us how to make a secure protocol feasible in real systems.

1.2 With Detection of Abnormalities

On the other hand, there are many solutions that aim to design networks and networking protocols based upon the detection of abnormalities, which is more or less a *reactive* approach. In general, these solutions are designed to be adaptive to any threats or abnormalities in the network. The solutions to this end can be classified as

- Statistical methods: The main idea is to let each node (e.g., sensor nodes) to compute a statistical digest of the monitored phenomenon over a moving window of recent readings. By utilizing the statistical digests to aid in decision making and data aggregation. Wireless nodes may be set in promiscuous mode by overhearing others' broadcast message. The results of statistical digests are then used as a *trust* measure for path selection or topology control.

For example, to measure the node's cooperativeness, it is possible to study the characteristics of misbehaving nodes on the network layer. Selfish nodes, for the sake of saving energy, usually refuse to forward data packets for other nodes. Malicious nodes may intentionally drop partial data packets in a random or periodic manner. A malicious node may also pretend to be adjacent to a node actually faraway from it, thus trap all packets destined to that node afterward. Thus, dropping "transient" packets is one of the most common characteristics of misbehaviors.

- Empirical benchmark: The main idea is to use empirical benchmark, represented by stochastic models or trace files. Currently, there is almost nothing existed for mobile ad hoc networks, even small-scale experiments [5]. Although many new attacks are proposed, the security effectiveness against these attacks remain at the level of discussions and security analysis, even not present in simulations for most of the work. This brings a lot of arguments in the course of justification.

2 Research Challenges

- *Threat models*: Wireless or sensor nodes may be compromised or physically captured. Adversaries can control the compromised nodes and gain access to secret information stored in them. Thus, they can launch multiple attacks like dropping or altering the message contents going through them, so as to prevent the sink from receiving authentic sensor readings. Also, there may be colluded attacks where two or more nodes collaborate to let the false reports escape detection in the downstream path to the sink.

- *Measurements and computation*: Once threats models are defined, the subsequent issue is how to measure or detect threats according to the threats models and the cost at which these measurements are collected and processed.

- *Performance*: While in the design of security solutions (network) performance might not be a focus, it is necessary to ensure that a security-oriented algorithm or protocol can be incorporated into a networking protocol without making severe performance degradation. This is a very challenging issue for detection of abnormalities which often time relies on a long-term observation.

Ideally, a powerful detection tool, similar to intrusion detection for the Internet, is expected.

References

[1] P. Lee, V. Misra, and D. Rubenstein, "Distributed Algorithm for Secure Multipath Routing," in *Proc. of IEEE INFOCOM'05*, March 2005.

[2] K. Sanzgir, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," *To Appear in IEEE Journal on Selected Areas of Communications (JSAC)*, 2005.

[3] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *To Appear in Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols.*, 2006.

[4] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks," tech. rep., UMBC and NIST, 2003.

[5] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-Based Evaluation: From Dependability to Security," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 48–65, 2004.

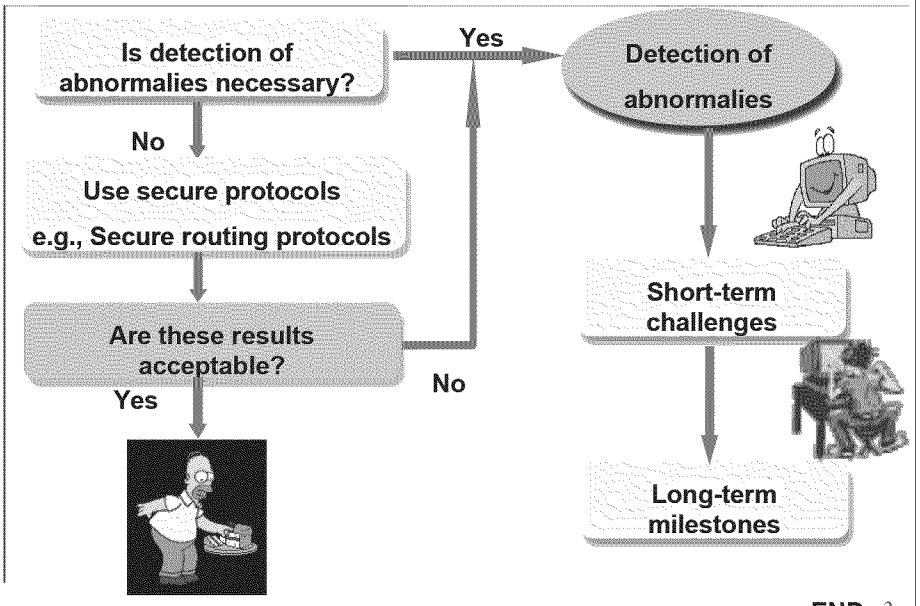
NC STATE UNIVERSITY

Detection of Abnormalies in MANETs

Wenye Wang

Department of Electrical and Computer Engineering
North Carolina State University

From Problems To Solutions



END 2

Secure Routing in MANETs

- Security is a goal:
  - Show how attacks against ad-hoc and sensor networks and analyze the security of routing protocols.
  - Design/examine attacks and countermeasures.
- Routing is a goal:
  - design or modify current routing protocols
  - add new security features to prevent routing from attacks and interruption.
- **Question: Are these solutions feasible (useful) for MANETs?**

SecAODV: An Example

Number of Packets	% Packet Loss		Total Time sec.		RTT(avg) (ms)	
	500 B	200 B	500 B	200 B	500 B	200 B
10	100	90	9.009	9.009		24.78
50	94	96	49.162	49.170	18.99	16.24
100	96	97	99.312	99.392	21.29	16.98

- Why? May be the results of one or more factors
  - Bugs in the code (open-source)
  - Optimization
  - Protocol design
- Implications

NC STATE UNIVERSITY

Detection Techniques

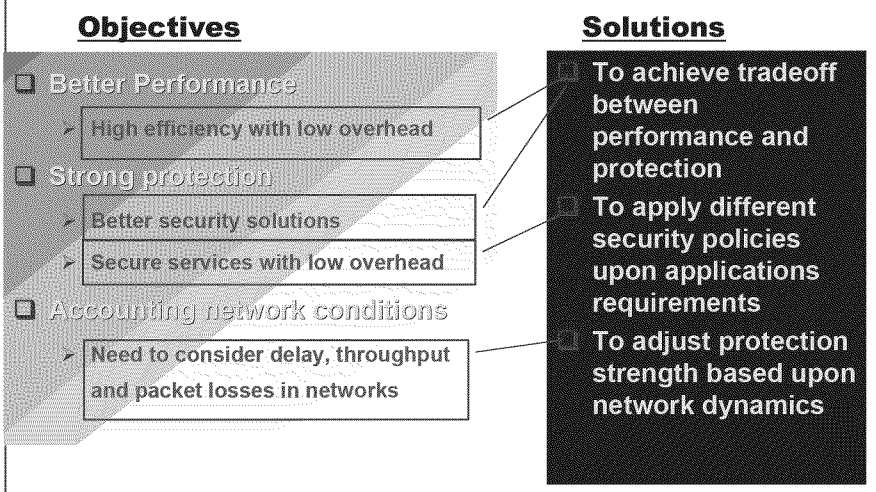
- Statistical methods
  - Compute statistical digests of trust values: e.g., selfish behaviors
  - Configure wireless nodes in promiscuous modes
  - Snoop transmissions of neighbors
- Model-based methods
  - Empirical benchmark
  - Stochastic models
  - Trace files

NC STATE UNIVERSITY

Short-Term Challenges

- Threats models
  - Basic functions: dropping/altering/injecting messages
  - Wireless or sensor nodes may be compromised or physically captures, what are the differences? As bad as malicious nodes?
- Measurements and computation
- Performance
  - Need to ensure that a security-oriented algorithm or protocol is applicable to a real system without severe performance degradation.
- **GOAL: Tunable protection**
  - Application- oriented
  - User preference

Take An Example in Wireless LANs



Security Policies

Type	Policies	Description
Individual Policies	No Security	When no security protocol is configured in test-bed.
	WEP Policies	Involve only WEP (40 bit key,128 bit key).
	IPSEC Policies	Involve IPSEC (3DES, MD5, SHA).
Hybrid Policies	IPSEC Policies	Involve IPSEC (3DES, MD5, SHA) and WEP.
	802.1x Policies	Involve 802.1x, Radius, EAP (MD5,TLS), IPSEC and WEP.

Experimental Results - *Authentication Time*

Policy (Hybrid Protocols)	With Roaming	
IPSEC	1.405s	1.432s
802.1x-EAP(MD5) without IPSEC	0.427s	1.749s
802.1x-EAP(M IPSEC		.749s
802.1x-EAP(TLS) without IPSEC		3.144s
802.1x-EAP(TLS) with IPSEC	3.117s	3.144s

802.1x-EAP(MD5) results in the *lowest* authentication time

IPsec provides a good tradeoff between security and overhead.

802.1x-EAP(TLS) causes the *longest* authentication time and higher data loss during handoff

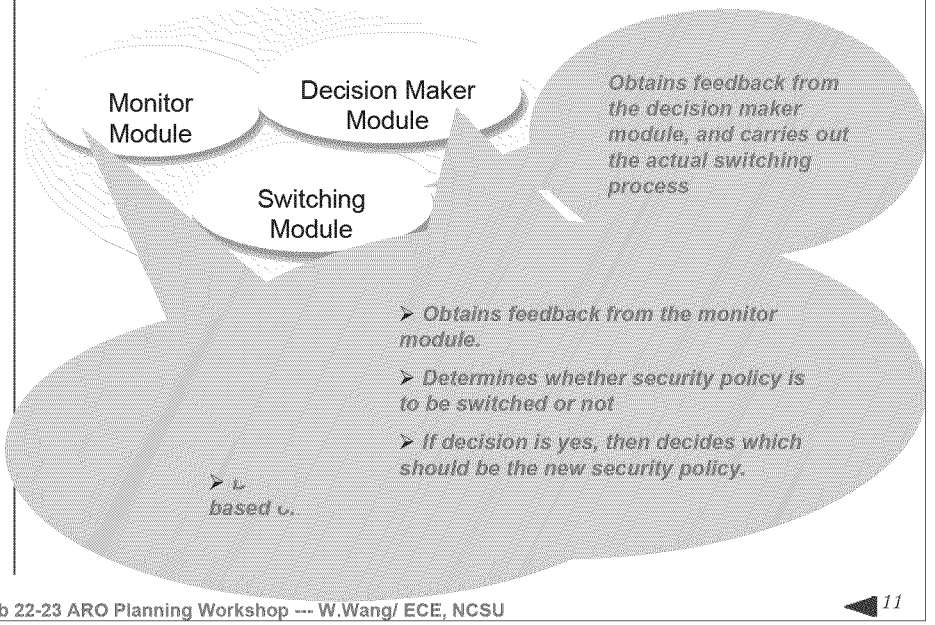
Experimental Results – *Delay with IPSec*

- Best network scenario: indoor, one-hop, single node
- Worst case delay

End-to-End Delay (msec)	Packet Size (bytes)				
	64	128	256	512	1024
No Security (> 5 times)	17.72	11.83	28.14	94.96	28.80
AES-SHA1 (>10 times)	90.718	61.63	67.11	408.12	715.75
AES-MD5 (20 times)	52.21	63.55	105.11	150.02	1012.06
3DES-SHA1	54.62	48.35	61.19	182.61	530.23
3DES-MD5	71.02	49.69	53.00	359.91	804.41

STEP2 -- Self-Tuned Protection and Performance Architecture

NC STATE UNIVERSITY



NC STATE UNIVERSITY

Long-Term Milestones

- Benchmark of threats models
  - 10 most commonly threats : spoofing of IP address, forging of route request, forging of route reply, injecting route reply without receiving a route request, replay attack, rushing attacks, generating false errors, jamming, man-in-the-middle attack, modifying node list on a route request.
  - Database with more threats
  - Selection of distributions
- Dynamic defense strategy upon detection of threats!

THANK YOU!